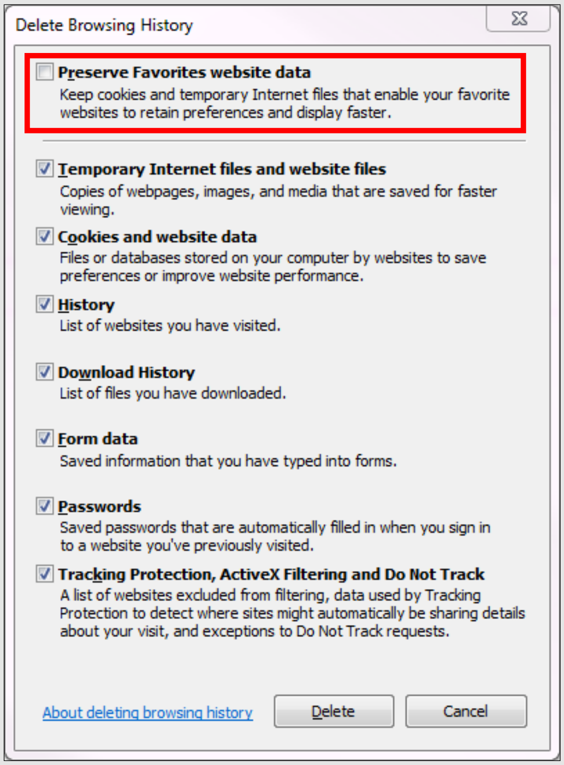
UPDATED AUG 2020

DELETE BROWSER ARTIFACTS SMART CARD

Browser Artifacts—Cookies, Cache & History

Information such as browsing history, cache, and cookies are saved on your computer while you surf the Web. They are used in various ways to improve your browsing experience. These private data components, while resulting in conveniences such as faster load times and auto-populated fields, can be used by nefarious actors. Whether it be the password for your email account or your credit card number and address, much of the data left behind at the end of your browsing session could be dangerous in the wrong hands. In order to protect yourself, we recommend you delete these artifacts on a regular basis.

Deleting Internet Explorer Web Browser Artifacts


Delete Browsing History

☐ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files and website files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies and website data**
Files or databases stored on your computer by websites to save preferences or improve website performance.

☑ **History**
List of websites you have visited.

☑ **Download History**
List of files you have downloaded.

☑ **Form data**
Saved information that you have typed into forms.

☑ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

☑ **Tracking Protection, ActiveX Filtering and Do Not Track**
A list of websites excluded from filtering, data used by Tracking Protection to detect where sites might automatically be sharing details about your visit, and exceptions to Do Not Track requests.

Make sure you are using the latest version of Internet Explorer (IE), IE 11.

Click the Settings ⚙ button on the top right.

Click "Internet Options".

Under the "General" tab, locate the "Browsing History" section.

Click "Delete".

You will see the window to the left. (A useful keyboard shortcut to access this window is "C*trl-Shift-Delete").*

Deselect "Preserve Favorites website data".

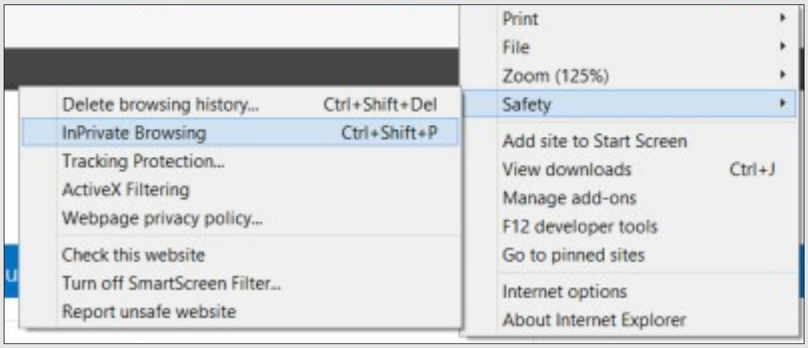
Select the boxes next to the history you want to remove and click "Delete".

Exit/quit all browser windows and re-open the browser.

Note: Internet Explorer is no longer supported on any mobile device.

As of March 2017, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default browser on its Windows 10 devices. As of February 2020, IE version 10 is no longer in support. If you are still using IE be sure to upgrade to IE 11.

Using Internet Explorer InPrivate Browser



To activate "InPrivate", click the Settings ⚙ button on the top right.

Click "Safety".

Click "InPrivate Browsing".

(Alternatively, after opening Internet Explorer you can use the shortcut "*Ctrl-Shift-P*").

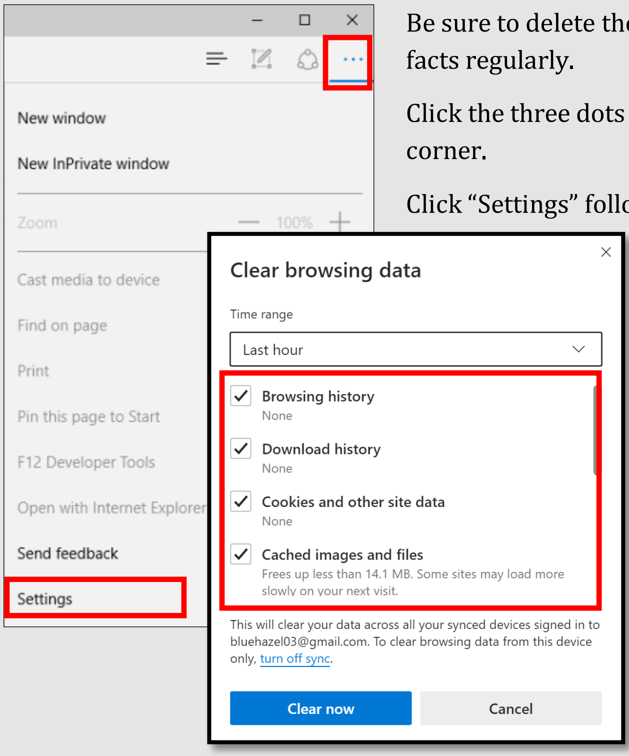
An internet cookie is a small piece of data sent from a website and stored on a user's computer while the user is browsing.

UPDATED AUG 2020

DELETE BROWSER ARTIFACTS SMART CARD

An internet cookie is a small piece of data sent from a website and stored on a user's computer while the user is browsing.

Deleting Microsoft Edge Web Browser Artifacts



Clear browsing data

Time range

Last hour

☑ Browsing history
None

☑ Download history
None

☑ Cookies and other site data
None

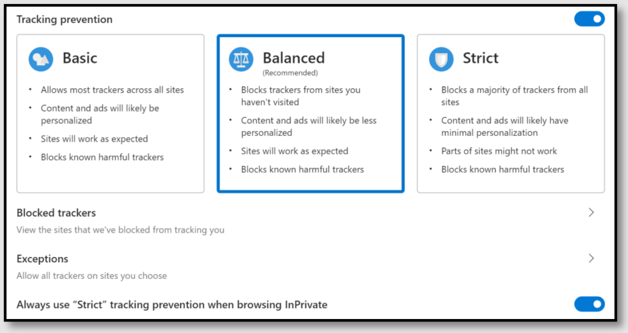
☑ Cached images and files
Frees up less than 14.1 MB. Some sites may load more slowly on your next visit.

This will clear your data across all your synced devices signed in to bluehazel03@gmail.com. To clear browsing data from this device only, turn off sync.

Be sure to delete the browser artifacts regularly.

Click the three dots at the top right corner.

Click “Settings” followed by the “Privacy & security” tab.



Tracking prevention

Basic
- Allows most trackers across all sites
- Content and ads will likely be personalized
- Sites will work as expected
- Blocks known harmful trackers

Balanced (Recommended)
- Blocks trackers from sites you haven't visited
- Content and ads will likely be less personalized
- Sites will work as expected
- Blocks known harmful trackers

Strict
- Blocks a majority of trackers from all sites
- Content and ads will likely have minimal personalization
- Parts of sites might not work
- Blocks known harmful trackers

Blocked trackers
View the sites that we've blocked from tracking you

Exceptions
Allow all trackers on sites you choose

Always use “Strict” tracking prevention when browsing InPrivate

Select “Tracking prevention,” recommend selecting the “Balanced” tracking selection.

Then click “Choose what to clear” under “Clear Browser Data”.

Select the boxes next to the history you want to remove and

Mobile Browser

Open the Edge browser.

Tap the menu button ☆ on the top right.

Tap to 🕓 view history.

Tap to 🗑 clear all history.

Choose the types of data to remove from your phone and tap “Clear”.

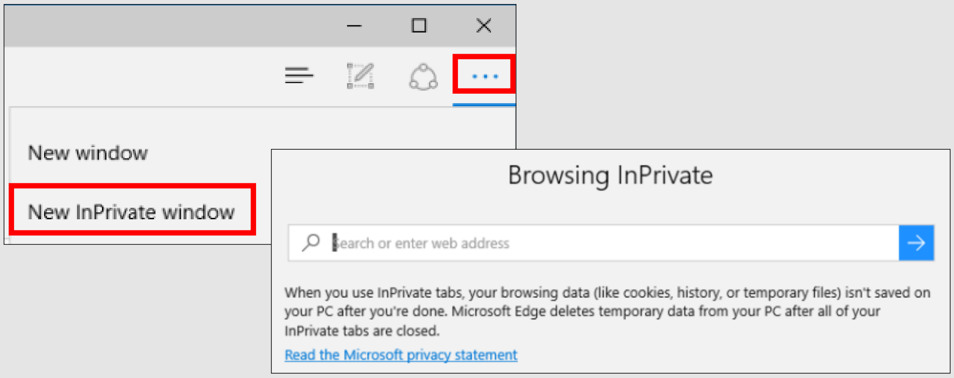
Using Microsoft Edge InPrivate Browsing

Edge is Microsoft's new browser that comes with Windows 10. It is meant to eventually replace IE.

Edge comes with an option called “InPrivate”, which is the browser's private mode that does *not* record your activities.

To activate “InPrivate”, click the three dots in the browser's upper right corner.

Click “New InPrivate window”.



Browsing InPrivate

Search or enter web address

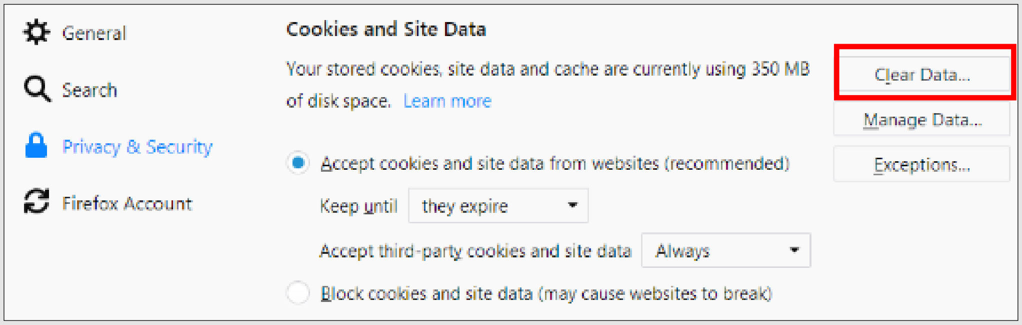
When you use InPrivate tabs, your browsing data (like cookies, history, or temporary files) isn't saved on your PC after you're done. Microsoft Edge deletes temporary data from your PC after all of your InPrivate tabs are closed.

Read the Microsoft privacy statement

UPDATED AUG 2020

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Firefox Web Browser Artifacts



Cookies and Site Data

Your stored cookies, site data and cache are currently using 350 MB of disk space. Learn more

● Accept cookies and site data from websites (recommended)

Keep until: they expire

Accept third-party cookies and site data: Always

○ Block cookies and site data (may cause websites to break)

Click the menu button at the top right and click “Options”.

Click “Privacy & Security” on the left.

Then click “Clear Data”.

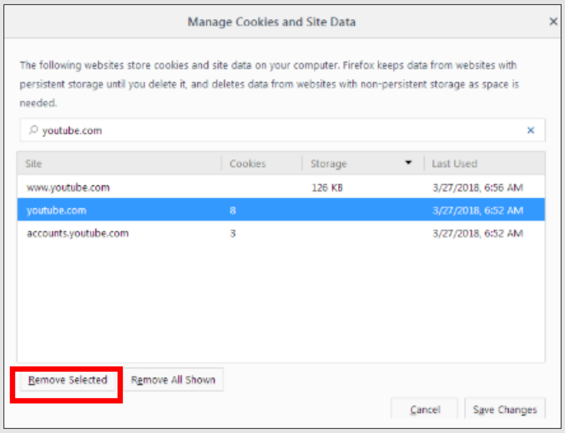
Individual Cookies

You can also remove individual cookies.

From the “Privacy & Security” screen, click “Manage Data”.

Select the site(s) you wish to clear data for.

Then click “Remove Selected”.



Manage Cookies and Site Data

The following websites store cookies and site data on your computer. Firefox keeps data from websites with persistent storage until you delete it, and deletes data from websites with non-persistent storage as space is needed.

youtube.com

Site	Cookies	Storage	Last Used
www.youtube.com		126 KB	3/27/2018, 6:56 AM
youtube.com	8		3/27/2018, 6:52 AM
accounts.youtube.com	3		3/27/2018, 6:52 AM

Mobile Browser

Tap the Menu icon on the top right.

Tap “Settings”. Scroll down to “Clear Private Data” and tap it.

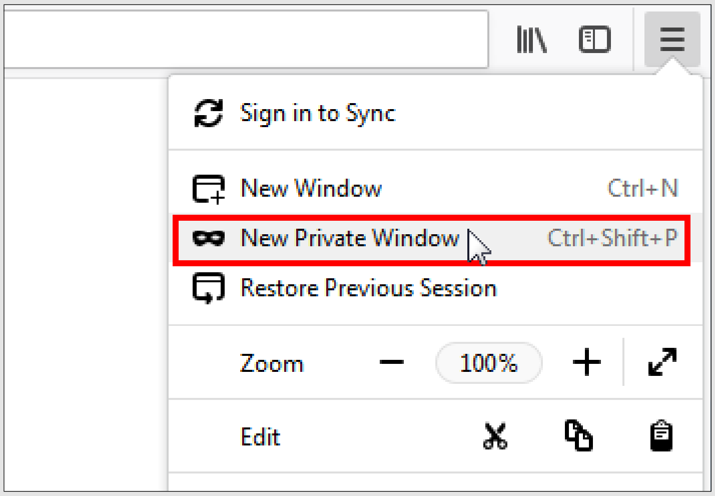
Selected data to be cleared. Tap “Clear Data.”

To manage how your data is shared and tracked, tap “Privacy” then tap “Tracking Protection” from the Settings menu.

“Enabled In Private Browsing” will inform sites that you do not want your browsing behavior tracked, but honoring this is voluntary.

Cookies can also be disabled from this screen.

Using Firefox Private Browsing Mode



To open a new Private Window, click the menu button on the top right.

Click “New Private Window”.

Alternatively, after opening Firefox you can use the shortcut “*Ctrl-Shift-P*”.

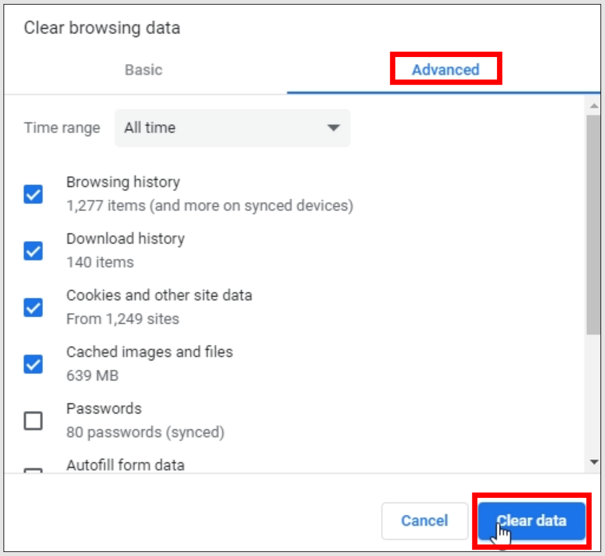
Important: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be installed on your computer.

Private Browsing also includes Tracking Protection, which prevents companies from tracking your browsing history across multiple sites.

DELETE BROWSER ARTIFACTS SMART CARD

Chrome doesn't have control over third party websites or their privacy practices, so be cautious when accessing websites.

Delete Google Chrome Browser Artifacts



Clear browsing data

Time range: All time

☑ Browsing history — 1,277 items (and more on synced devices)

☑ Download history — 140 items

☑ Cookies and other site data — From 1,249 sites

☑ Cached images and files — 639 MB

☐ Passwords — 80 passwords (synced)

☐ Autofill form data

Individual Cookies

You can also remove individual cookies.

Click the ⋮ icon at the upper right corner.

Click “Settings”.

Click the “Advanced” button on the left hand side.

Under the “Privacy & Security” section, click the “Site Settings”.

Click “Cookies and site data” and then “See all cookies and Data”.

Click 🗑 for the sites you wish to clear.

Click the ⋮ icon at the upper right corner.

Click “History” or hold *Ctrl-H*.

Click “History” again on the menu on the upper left hand side.

Click “Clear Browsing Data”. You can also hold C*trl-Shift-Delete*.

Click the “Advanced” tab in the pop-up window.

Select the Time range you desire.

Select the boxes next to the history you want to remove and click “Clear Browsing Data”.

Exit/quit all browser windows and re-open the browser.

Mobile Browser

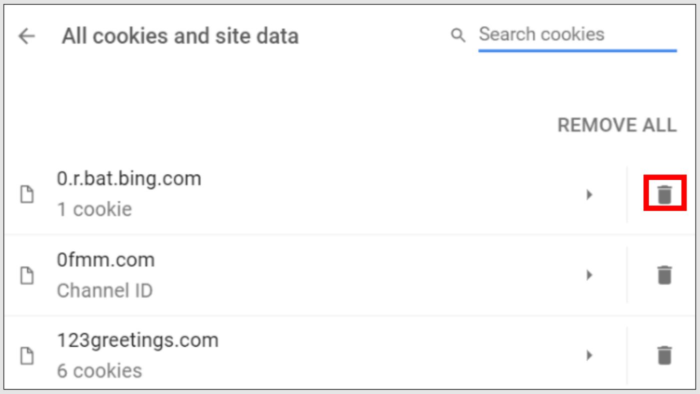
Tap the menu ⋮ icon.

Then tap “Settings”.

Tap “Privacy”.

Tap “Clear Browsing Data”.

Select the boxes next to the history you want to remove and tap “Clear Data”.



All cookies and site data

0.r.bat.bing.com	1 cookie
0fmm.com	Channel ID
123greetings.com	6 cookies

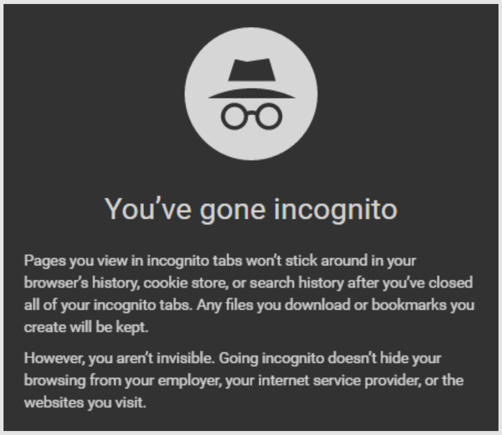
Using Google Chrome Incognito Mode

Chrome’s Incognito mode will *not* save a record of what you visited or downloaded.

Be aware that Incognito is not available if you are using Window 10’s “Family Mode.”

Click the ⋮ icon at the upper right. Select “New Incognito Window”.

You can also use Incognito via the Chrome app on your iOS or Android device. Follow the same steps as above with the app.



You’ve gone incognito

Pages you view in incognito tabs won’t stick around in your browser’s history, cookie store, or search history after you’ve closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

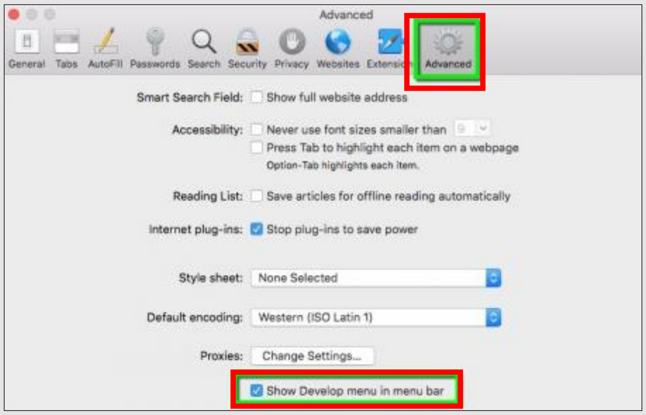
However, you aren’t invisible. Going incognito doesn’t hide your browsing from your employer, your internet service provider, or the websites you visit.

Like Microsoft Edge’s InPrivate Browser, Chrome’s Incognito will require you to constantly type in your password for logins. So you may prefer to use the regular Google Chrome browser out of convenience.

UPDATED AUG 2020

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Safari Browser Artifacts



Smart Search Field: □ Show full website address

Accessibility: □ Never use font sizes smaller than 9
□ Press Tab to highlight each item on a webpage
Option-Tab highlights each item.

Reading List: □ Save articles for offline reading automatically

Internet plug-ins: ☑ Stop plug-ins to save power

Style sheet: None Selected

Default encoding: Western (ISO Latin 1)

Proxies: Change Settings...

☑ Show Develop menu in menu bar

Click the “Safari” menu on the top left.

Click “Preferences”.

Click the “Advanced” tab.

Check the box at the bottom for “Show Develop menu in menu bar” and close the window.

Click the “Develop” menu at the top and click “ Empty Caches”.

Then click the “History” menu at the top and click “Clear History”.

Right click on the Safari icon in your App tray and select “Quit”.

Mobile Browser

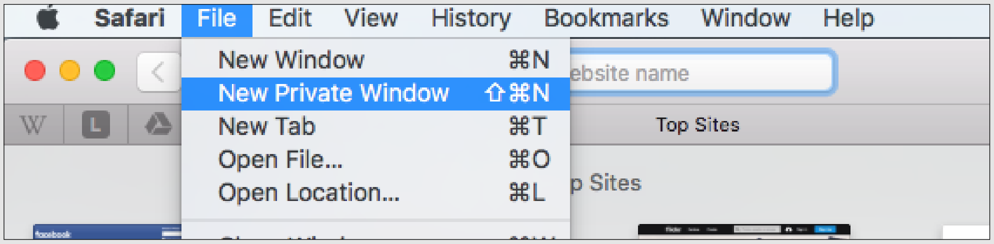
Open your iOS Settings app.

Scroll down and tap “Safari”.

Tap the “Clear History and Website Data” link in blue.

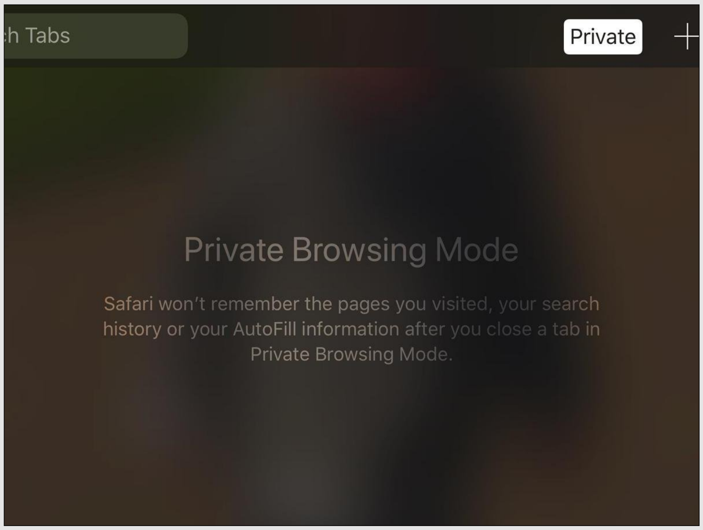
Exit/quit all browser windows and re-open the browser.

Deleting Safari Browser Artifacts



To open a Private Window, click “File” on the top left.

Click “New Private Window”.



Private Browsing Mode

Safari won't remember the pages you visited, your search history or your AutoFill information after you close a tab in Private Browsing Mode.

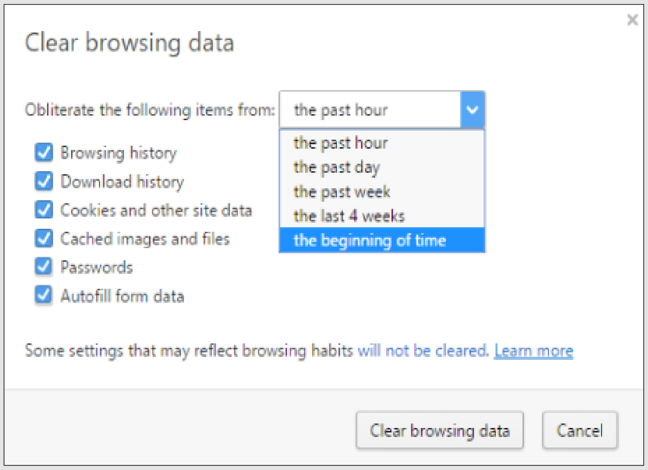
Enabling Private Browsing limits Safari in three important ways: It prevents the browser from creating a history of the pages you visit, it stops AutoFill information like website usernames and passwords from being remembered, and any tabs you open won't be stored in iCloud.

Safari automatically prevents cross-site tracking, and requests that sites and third-party content providers don't track you as a rule. Additionally, the privacy mode stops sites from modifying any information stored on your iOS device, and deletes cookies when you close the associated tab.

When you are on a website that uses Apple Pay, the site can automatically check if you have Apple Pay set up if you haven't disabled this feature.

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Opera Browser Artifacts



Clear browsing data

Obliterate the following items from: the past hour

- the past hour
- the past day
- the past week
- the last 4 weeks
- the beginning of time

☑ Browsing history
☑ Download history
☑ Cookies and other site data
☑ Cached images and files
☑ Passwords
☑ Autofill form data

Some settings that may reflect browsing habits will not be cleared. Learn more

Clear browsing data | Cancel

Click the "Menu" button on the top left.

Click "History".

Click "Clear Browsing Data".

Select the Time frame and the boxes next to the history you want to remove and click "Clear Browsing Data." Selecting "Advanced" will provide the user with more options to clear.

Exit/quit all browser windows and re-open the browser.

Mobile Browser

Tap on the "Menu" button.

Tap "History".

Tap "Clear All".

Tap "Yes" to confirm.

Using a Private Tab in Opera Browser

Opera's Private Tab browsing deletes browsing history, cache, cookies, and logins when you close the tab.

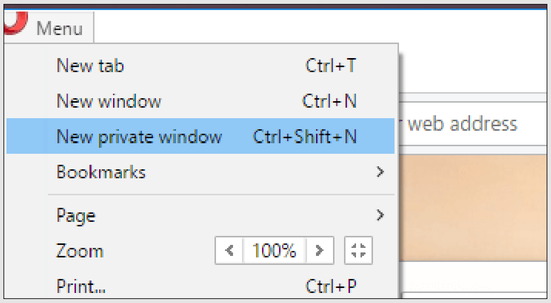
Please note that if you deliberately save data, such as a bookmark or a file, it will still be visible after the tab is closed.

You may prefer to use the regular Opera Browser window out of convenience. Be sure to delete browser artifacts regularly.

To create a Private Tab, click the "Menu" button on the top left corner.

Click "New Private Window".

Private browsing is also available on Opera Mini mobile browser as well.



Privacy is about much more than "hiding things". It's about protection. #ProtectYourPrivacy

DELETE BROWSER ARTIFACTS SMART CARD

Privacy and Security-Related Browser Tools

GHOSTERY

Ghostery is a German-owned freeware browser extension that allows you to choose what to block, on a tracker-by-tracker or site-by-site basis, or a combination of the two.

The tool also offers tracker profiles so you can learn about the companies collecting data on you as you browse the web.

Ghostery looks at the HTML code on each web page you visit to see if there are “tags” or “trackers” placed by a company that works with the website. The tool can determine if the company is showing you ads, collecting data, or giving you added functionality on the page.

The extension is available for Firefox, Chrome, Safari, Internet Explorer, Microsoft Edge, and Opera. It is also accessible via a mobile application for Android, iOS, and Firefox for Android.

BLUR

Blur protects your passwords, payments, and privacy from cyber criminals.

The US-based tool masks your passwords, email addresses, credit card numbers, and address information. It also has the ability to create strong passwords for new and existing accounts.

Blur blocks hundreds of companies from collecting your data online and blocks tracking that doesn’t rely on cookies.

Free and Premium versions are available. Masked credit card is only available with the Premium version which costs $39/year (Basic), $14.99/month (Unlimited), or $99/year (Unlimited). This extension is available for Chrome, Firefox, Safari, Opera, Internet Explorer, Android, and iOS.

ABP

AdBlock Plus is a German-based extension that blocks banner ads, pop-up ads, rollover ads, and more. It stops you from visiting known malware-hosting domains and disables third-party tracking cookies and scripts. It can even block video ads on Facebook and YouTube.

This extension works for Android, Chrome, Firefox, Internet Explorer, Opera, Safari, Microsoft Edge and Yandex.

D.
DISCONNECT

Disconnect is a smart filter that stops third-party sites from tracking you. The companies that are collecting your information are shown in real-time as pages load. You can even see how those sites may be linked to other sites that track information.

Disconnect encrypts the data you exchange with common sites and helps to prevent visiting sites that have malware.

The extension is available for Chrome, Firefox, Safari, and Opera.

Before installing an add-on or extension, review the requested permissions. They may request to access and store to your data.